ABSTRACT

A method and apparatus for memory encryption with reduced decryption latency. In one embodiment, the method includes reading an encrypted data block from memory. During reading of the encrypted data block, a keystream used to encrypt the data block is regenerated according to one or more stored criteria of the encrypted data block. Once the encrypted data block is read, the encrypted data block is decrypted using the regenerated keystream. Accordingly, in one embodiment, encryption of either random access memory (RAM) or disk memory is performed. A keystream is regenerated during data retrieval such that once the data is received, the data may be decrypted using a single clock operation. As a result, memory encryption is performed without exacerbating memory latency between the processor and memory.